IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

UNITED STATES OF AMERICA	)	
	)	
	)	**Case No. 3:19cr130**
	)	
OKELLO T. CHATRIE,	)	
Defendant	)	

DEFENDANT OKELLO CHATRIE'S SUPPLEMENTAL MOTION TO SUPPRESS EVIDENCE OBTAINED FROM A "GEOFENCE" GENERAL WARRANT

Okello Chatrie, through counsel, submits this supplement to his motion to suppress all evidence and fruits obtained from a "geofence" general warrant, ECF No. 29, pursuant to the Court's Order entered on May 13, 2020. *See* ECF No. 103.

INTRODUCTION

This case turns on a novel and invasive form of electronic surveillance, a so-called "geofence" warrant, involving the search of "numerous tens of millions" of Google users to generate a single investigatory lead. *See* ECF No. 96-1 at 4. Local police had no suspects in the robbery of the Call Federal Credit Union, so they decided to enlist Google to sleuth for them. Investigators went to a Virginia magistrate and, without conveying critical information, obtained a staggeringly broad and unparticularized warrant to go fishing in a pool of private location data that most people have never heard of. They demanded the location information associated with all Google users who happened to be in the vicinity of the bank during rush hour on a Monday evening, and thus, caused Google to search numerous tens of millions of accounts at their behest.

The basic facts involved are found in Mr. Chatrie's initial motion to suppress, *see* ECF No. 29 at 4-7. In short, the warrant followed a three-step process Google developed: "Step One" required Google to search all user accounts and provide "anonymized information" about any

devices in the area during the 30 minutes on either side of the robbery. In response, Google searched every user with "Location History" enabled and estimated that 19 devices were within 150 meters of the bank during that one-hour timeframe. Next, in "Step Two," investigators were to cull the list from Step One, after which Google would produce additional, "anonymized" location information about devices of interest for one hour on either side of the robbery (*i.e.*, two hours total), without geographic restriction. But instead of culling the list, investigators demanded additional information on all 19 devices—multiple times. Google did not comply until investigators identified a subset of nine users for further scrutiny. Finally, at "Step Three," investigators narrowed the list to three devices of interest and obtained de-anonymized information about those Google users. One of the three devices belonged to Mr. Chatrie, who became the government's primary suspect. As the government agrees, *see* 1/21/20 Tr. at 172-73, all of the evidence implicating Mr. Chatrie in this crime emanates from this Google geofence search.

From the beginning, Mr. Chatrie has urged this Court to find that such a warrant is unconstitutional, both categorically and on the facts of this case, because it is fatally overbroad and lacks the particularity required by the Fourth Amendment. *See* ECF No. 29 at 3. Since Mr. Chatrie made his initial motion to suppress, however, Google has filed an *amicus* brief and two affidavits that clarify and magnify the scope of the privacy intrusion worked by the government in this case. *See* ECF Nos. 59-1 & 96. The Court also heard testimony from a digital forensics expert, Spencer McInvaille. *See* 1/21/20 Tr. Mr. Chatrie sought leave to file a supplemental motion and present these new facts to the Court in advance of further testimony and argument, and in support of his motion to suppress all evidence obtained from the geofence warrant, as well as all fruits thereof. The Court granted Mr. Chatrie's request and subsequently extended the filing deadline to May 22, 2020. *See* ECF Nos. 101 & 103.

Mr. Chatrie had a reasonable expectation of privacy in his Google Location History records. As the Supreme Court recently recognized in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), such data is capable of revealing the "privacies of life" and is therefore constitutionally protected. *Id.* at 2214. It can reveal who is inside a home, church, or hotel—all of which are implicated here. The ability to access this Google data grants the government unprecedented surveillance powers, enabling investigators to locate individuals quickly, cheaply, and retroactively. This may be a boon to law enforcement, but it is also a Fourth Amendment search, just as it was in *Carpenter*. *Id* at 2230.

The so-called "third-party doctrine" does not apply to Location History records, and therefore a *valid* warrant—*i.e.*, one that is properly particularized and supported by probable cause—should be required in order for law enforcement to access it.

Location History records are qualitatively different than the "business records" that have fallen into the traditional third-party exception, such as bank deposit slips or telephone numbers dialed. *See United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979); *see also Carpenter*, 138 S. Ct. at 2216–17. As the Supreme Court has recently and repeatedly articulated, digital is different. *See id.* at 2214; *Riley v. California*, 573 U.S. 373, 393 (2014) (comparing a physical search to the search of a cell phone is like "saying a ride on horseback is materially indistinguishable from a flight to the moon"); *United States v. Jones*, 132 S. Ct. 945, 957 (2012) (the third-party doctrine is "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks") (Sotomayor, J., concurring). As a result, any extension of old rules to digital data "has to rest on its own bottom." *Riley*, 134 S. Ct. at 2489.

In this case, Mr. Chatrie did not "voluntarily" convey his cell phone location data to Google in any meaningful way. Like many Google users, he did not knowingly or intentionally "opt-in" to Google's Location History service. And like the cell site location information in *Carpenter*, his Location History data is not subject to the third-party doctrine.

While the government obtained a warrant in this case, it did not obtain one for Mr. Chatrie's Location History data. In fact, it did not seek anyone's data in particular. Rather, the government compelled Google to search *everyone's* data in order to develop an investigative lead. This warrant was unconstitutional. It was both overbroad and lacking in particularly, a forbidden general warrant purporting to authorize a dragnet search of Google users. It did not—and could not—satisfy the Fourth Amendment's probable cause and particularity requirements, rendering it wholly impermissible and void from the beginning. Indeed, it was so deficient that no objectively reasonable officer could rely on it, and as a result, Mr. Chatrie asks this Court to suppress all evidence obtained as a result, as well as all fruits of the poisonous tree.

NEW FACTS

Mr. Chatrie initially characterized the geofence warrant in this case as "a general warrant purporting to authorize a classic dragnet search of every Google user who happened to be near a bank in suburban Richmond during rush hour on a Monday evening." ECF No. 29 at 3. At the time, Mr. Chatrie understood this search to encompass "a trove of private location information belonging to 19 unknown Google users" who were within 150 meters of the bank. *Id.* But that, it turns out, was just the tip of a gargantuan iceberg. As Google now explains, the geofence search involved not just 19 users near the bank, but "roughly one-third of active Google users (i.e., numerous tens of millions of Google users)." ECF No. 96-1 at 3.

Geofence warrants differ from other types of law enforcement requests, entailing a uniquely broad search of all Google users who have "Location History" enabled on their devices. *See* ECF No. 59-1 at 11. Whereas typical requests compel Google to disclose information associated with a specific user, "[g]eofence requests represent a new and increasingly common form of legal process that is not tied to any known person, user, or account." *Id*; *see also* 1/21/20 Tr. at 21. Here, the warrant did not identify Mr. Chatrie in any way. Nor did it identify any of the users whose personal information was searched and turned over to law enforcement. Instead, the warrant operated in reverse: it required Google to identify users with Location History records and then allowed police full discretion to cull through this private information for devices of interest.

Geofence warrants require Google to produce data regarding all Google users who were within a geographic area during a given window of time. But, as Google explains, there is "no way to know ex ante which users may have [Location History] data indicating their potential presence in particular areas at particular times." *Id.* at 12. Thus, in order to comply with the request, Google must "search across all [Location History] journal entries to identify users with potentially responsive data, and then run a computation against every set of coordinates to determine which [Location History] records match the time and space parameters in the warrant." *Id.* at 12-13.

Location History records are one of three types of user location information maintained by Google. If a user has the Google Location History service enabled, then Google estimates the user's device location using GPS signals, signals from nearby Wi-Fi networks, Bluetooth beacons, or cell phone towers. *See* ECF 96-1 at 4. Google saves this information on a map in each user's "Timeline," *id.* at 2, which Google describes as a "digital journal" of a user's locations and travels. *See* ECF No. 59-1 at 16. Google considers this information to be communications "content" for

purposes of the Stored Communications Act, 18 U.S.C. § 2703, requiring the government to obtain a warrant supported by probable cause in order to access it. *See id*.

In addition to Location History records, Google maintains separate databases for user location information derived from two other Google services: "Web & App Activity" and "Google Location Accuracy." Web & App Activity is on by default and it saves location information generated from activities like running a Google Search or using a Google application such as Google Maps, Gmail, or YouTube. *See* ECF No. 96-1 at 5; 1/21/20 Tr. at 23; *In Re Google Location History Litigation*, No. 5:18-cv-05062-EJD (N.D. Cal. Dec. 19, 2019). Google uses this data to provide "a more personalized experience" through "faster searches and more helpful app and content recommendations." ECF No. 96-1 at 5. Google asserts that it did not search the Web & App Activity database in this case because that database does "not store a user's location at a level of detail precise enough to be responsive to a geofence warrant."[1]

Google Location Accuracy, formerly known as "Google Location Services," works on Android devices and is also enabled by default. It estimates a device's location using GPS data, Wi-Fi access points, Bluetooth sensors, and mobile network information. *See* ECF No. 96-1 at 6; 1/21/20 Tr. at 23. Google uses this information to improve location accuracy by estimating the physical location of Wi-Fi access points, Bluetooth beacons, and cell phone towers based on the GPS coordinates transmitted by devices that interact with those networks. *See* ECF No. 96-1 at 6-7; 1/21/20 Tr. at 64-65. "In other words," explains Google, "[Google Location Accuracy] data might be used by the device to calculate a location data point that is stored in [Location History.]"

[1] Google states that Web & App Activity data "reflects a device's location to an approximate area of at least one square kilometer" and is "therefore too coarse to be responsive to the warrant," which initially entailed a search area with a 150-meter radius. ECF No. 96-1 at 8.

Id. at 6.[2] Google asserts, however, that it did not directly search the Google Location Accuracy database in response to the geofence warrant because the data is "not stored with user identifiers" and is "used in an anonymous way." *Id.*

Thus, even though the geofence warrant required Google to produce location data for "each type" of Google account inside the geofence, *see* ECF No. 54-1 at 4, 9, Google did not do so. Instead, Google says that it only searched the Location History database, not the Web & App Activity or Google Location Accuracy databases. *See* ECF No. 59-1 at 12; ECF No. 96-1 at 7-8. According to Google, Location History is the only form of data that is "sufficiently granular" and searchable to be responsive to a geofence request. ECF No. 96-1 at 7.

Consequently, Google did not search the contents of every Google user in order to respond to the warrant. Instead, it searched those users with Location History enabled on their accounts—*i.e.*, the "Sensorvault." But this is no small number. It amounts to "roughly one-third of active Google users." *Id.* at 4. Not even Google, however, knows precisely how many users it searched in this case. *Id.* Rather, Google estimates that "numerous tens of millions of Google users" had Location History enabled in 2019, all of whom had their accounts searched in order to identify 19 users who were, perhaps, roughly within 150 meters of the bank. *Id.*[3]

Of critical importance is that, in practice, the effective range of the geofence was more than double 150 meters. As a result, at least some of the 19 users identified by Google were likely never within the 150-meter geofence at all. As Google states, "it is possible that when Google is

[2] When estimating a user's location through the Location History service, Google appears to use historical location data from other users, stored in the Google Location Accuracy database, to estimate a device's likely GPS coordinates based on the presence and strength of known nearby Wi-Fi, Bluetooth, and cell phone tower signals. For example, if many devices transmit a similar set of GPS coordinates when they "see" a particular Wi-Fi network, then Google may attribute those GPS coordinates to a device that later "sees" the same Wi-Fi network if GPS is unavailable for that device.

[3] Thus, assuming Google has two billion active users, a third of which is 660 million (*i.e.*, twice the population of the United States), then 19 users represent a hit rate of 0.0000029%.

compelled to return data in response to a geofence request, some of the users whose locations are estimated to be within the radius described in the warrant (and whose data is therefore induced in a data production) were in fact located outside the radius." *Id*. at 9; *see also* ECF No. 59-1 at 20 n.12 (estimates may include "false positives—that is, that [they] will indicate that certain Google users were in the geographic area of interest to law enforcement who were not in fact there."); 1/21/20 Tr. at 65. This phenomenon is a product of how Google calculates a user's location based on "multiple inputs," including the strength of nearby Wi-Fi signals. ECF No. 96-1 at 8; *see also supra* n.2. According to Google, the latitude/longitude coordinates saved in Location History records do not necessarily reflect a user's actual location, *id.*, but are "probabilistic estimates," each with a different "margin of error." ECF No. 59-1 at 10 n.7. Google presents that margin of error as a "Map Display Radius," which is often depicted on a map as a shaded blue circle extending outwards from the "blue dot" indicating the user's estimated location. ECF No. 96-1 at 9. Importantly, there is only an "estimated 68% chance that the user is actually within the shaded circle surrounding that blue dot." *Id.* Or in other words, chances are better than 1-in-5 that the user is outside of the shaded circle altogether.[4]

Google has provided numerical values for the margins of error in this case, the largest of which is 387 meters from coordinates near the center of the 150-meter geofence. *See* ECF No. 68 Ex. A at 6-12, 17-37. Figure 1, below, depicts the 150-meter geofence in red and the 387-meter margin of error in yellow. That margin of error indicates that at least one user[5] could have been more than 387 meters away from the bank—and more than 237 meters outside the geofence—but

[4] The size of the margin of error depends on the user location data available to Google. For example, coordinates obtained from GPS signals are more accurate than coordinates derived from Wi-Fi signals. *See* 1/21/20 Tr. at 64. In this case, 88% of the coordinates at issue were derived from Wi-Fi signals, as opposed to GPS. *Id.* None were derived from Bluetooth or cell phone tower data.

[5] "Device ID" number 702354289.

was nonetheless swept into the dragnet. In fact, Google is only 68% confident that the user was not even farther away than 387 meters. Put it another way, the yellow line indicates the minimum effective range of the geofence in this case, which is more than twice what the warrant authorized.

Figure 1

The true reach of the geofence, therefore, included not only a major thoroughfare (U.S. Route 360), the bank, and the Journey Christian Church, but also another road next to the church, a Ruby Tuesday restaurant, a Hampton Inn hotel, a mini storage facility, an apartment complex for seniors, and another residential apartment complex. *See* Tr. 1/21/20 at 66-67. Numerically, the 150-meter radius covered an area of 78,000 square meters, or about 17 acres, whereas the effective range was 470,000 square meters, or about 116 acres—an increase of more than 500 percent.

ARGUMENT

Execution of the geofence warrant was an unconstitutional search that intruded upon Mr. Chatrie's reasonable expectation of privacy in his Google location data. As Mr. Chatrie contends, the warrant was invalid because it was a general warrant, fatally overbroad and devoid of particularity, and therefore impermissible under the Fourth Amendment. *See* ECF No. 29 at 7, 16-24. Moreover, the warrant was *void ab initio*—so obviously deficient from the beginning that the search must be regarded as warrantless. As a result, the good-faith doctrine does not apply and the results of the search, including all of its fruits, should be suppressed.

I. The Geofence Warrant Intruded on Mr. Chatrie's Reasonable Expectation of Privacy in His Location History Records.

As Mr. Chatrie argues in his initial motion to suppress, the Supreme Court's recent decision in *Carpenter* applies to mobile location data obtained from Google just as much as similar data obtained from a cellular service provider. *See* 138 S. Ct. 22; ECF No. 29 at 7-11. Narrowly construed, *Carpenter* found a reasonable expectation of privacy in seven days of historical cell-site location information ("CSLI"), *id*. at 2217, because seven days was the shortest amount of time on the record before the Court. *See* ECF No. 48 at 2-4. Nonetheless, *Carpenter's* reasoning applies with at least equal force here. As Justice Gorsuch noted in dissent, presciently: "[W]hat distinguishes historical data from real-time data, or seven days of a single person's data from a download of *everyone*'s data over some indefinite period of time? . . . On what possible basis could such mass data collection survive the Court's test while collecting a single person's data does not?" *Id.* at 2267 (emphasis in original). The government struggles to argue that technical differences compel a different conclusion here, but Justice Gorsuch is correct. There are no principled distinctions to be had.

The government's primary objection centers on the length of the search, which covered two hours during rush hour on a Monday evening in Richmond, as opposed to the seven days at issue in *Carpenter*. But by "declin[ing] to determine whether there is a 'limited period' for which the government can acquire cell phone location information without implicating the Fourth Amendment," ECF No. 41 at 7, the Supreme Court did not give the government a free pass to obtain less than seven days of location data without a warrant. (In fact, the government's demand for seven days of data in *Carpenter* netted only two days of data. *See* 138 S. Ct. at 2212.)

On the contrary, the Supreme Court has repeatedly expressed concern that even short-term location tracking may constitute a search. *See Jones*, 565 U.S. at 415 (Sotomayor, J., concurring); *accord Carpenter*, 138 S. Ct. at 2215. Indeed, there are significant privacy implications involved in just a single trip to "the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour-motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on." *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring) (quoting *People v. Weaver*, 12 N.Y.3d 433, 441-442 (2009)). And this is especially true where the search reveals information about the interior of a constitutionally-protected space, such as a home. *See United States v. Karo*, 468 U.S. 705, 716 (1984) (finding that the use of a beeper to track a drum of chemicals into a private residence was a search); *see also Kyllo v. United States*, 533 U.S. 27, 37 ("The Fourth Amendment's protection of the home has never been tied to measurement of the quality or quantity of information obtained."). Such intrusions are "presumptively unreasonable in the absence of a search warrant." *Katz v. United States*, 389 U.S. 347, 361 (1967); *Kyllo*, 533 U.S. at 31 ("'At the very core' of the Fourth Amendment 'stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.'") (quoting *Silverman v. United States*, 365 U.S. 505 (1961)).

In this case, the geofence search revealed Google users who were not only inside the bank, but also in nearby homes, apartment complexes, and, it would seem, the Journey Christian Church. *See* 1/21/20 Tr. at 80-82 (describing the data for "Mr. Green," which begins at a hospital, ends at a private residence, and incorrectly indicates he went into church); *id.* at 83-85 (describing the data for "Mr. Blue," which shows a trip to a private residence with start and end points in an apartment complex); *id.* at 88-90 (describing the data for "Ms. Yellow," which shows a trip from a single-family residence to Manchester High School, followed by two local businesses, and then a return trip home). While this data was supposedly "anonymized" by Google, the defense was able to ascertain the likely identities of Mr. Green, Mr. Blue, and Ms. Yellow based upon the addresses of the residences involved, their travel history, and other publicly available information. *See id.* at 83, 87-88, 90-91.

Google's handling of the data at issue lends further credence to the notion that any slice of Location History data is private, no matter how small. Google considers Location History to be communications "contents" for purposes of the Stored Communications Act, 18 U.S.C. § 2703, meaning that from a privacy perspective, it is on par with the contents of an email or personal documents stored remotely on Google Drive. *See* ECF No. 59-1 at 9, 17; ECF No. 72 at 3. Far from an ordinary "business record," Google considers Location History to be a "digital journal" of users' movements and travels. ECF No. 59-1 at 16. As a result, Google requires the government to obtain a warrant supported by probable cause in order to access Location History records. *Id.* at 15-18. There is no exception for two hours of private, invasive data.

Finally, Location History records are at least as accurate as the cell site location information ("CSLI") in *Carpenter*, and equally capable of revealing the "privacies of life." 138 S. Ct. at 2217. Initially, Mr. Chatrie argued that all of the records in this case were "more precise than the cell site

location at issue in *Carpenter*." ECF No. 29 at 12. But as Google's *amicus* brief makes clear, Google derives Location History coordinates from "multiple inputs," some of which are more accurate than CSLI and some of which are not. ECF 96-1 at 4. These "inputs" include GPS signals, which are highly accurate and can estimate a device's location within "approximately twenty meters or less." *Id*. But they may also include Wi-Fi, Bluetooth, and CSLI data, which is generally less accurate than GPS. *Id*. Google explains that "[c]ombined, these inputs . . . can be capable of estimating a device's location to a higher degree of accuracy and precision than is typical of CSLI." *Id*.[6]

Nonetheless, Location History is at least as accurate as CSLI, *i.e.*, the least accurate "input" that Google uses. Furthermore, the *Carpenter* Court equated CSLI and GPS for purposes of Fourth Amendment analysis. *See* 138 S. Ct. at 2217 ("As with GPS information, the time-stamped [CSLI] data provides an intimate window into a person's life, revealing . . . his particular movements") (internal citation omitted). And as *Carpenter* instructs, courts should anticipate advances in the accuracy of such technologies in order to "'assure [ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" 138 S. Ct. at 2214 (quoting *Kyllo v. United States*, 533 U.S. 27, 34 (2001)) (alteration in original); *accord United States v. Jones*, 565 U.S. 400, 406 (2012). When new technologies "encroach upon areas normally guarded from inquisitive eyes," *id.*, courts must remain vigilant "to ensure that the 'progress of science' does not erode Fourth Amendment protections." *Id.* at 2223. Indeed, not even the government finds a meaningful difference between CSLI and GPS, conceding that *Carpenter* "t[ook] account of

[6] At the same time, however, because Location History was developed for the purpose of targeting customer advertisements and not for impeccable surveillance, estimates based on CSLI or Wi-Fi signals may be far less accurate than estimates based on GPS tracking. Consequently, a geofence search may mistakenly identify some users as being within the radius who were in fact located outside of it. *Id.* at 9. In the case, Google appears to have identified at least one user inside the Journey Christian Church who was likely never in the church at all, and may in fact have been more than 387 meters away. *See supra* at 9-10.

more sophisticated systems" and recognized that CSLI "is rapidly approaching GPS-level precision." ECF No. 41 at 8.

In this case, the Location History records produced by Google involve a mix of GPS and Wi-Fi inputs, with approximately 12% coming from GPS and 88% coming from Wi-Fi signals. *See* 1/21/20 Tr. at 64. But the government did not and could not—because of the nature of the colossal search Google conducts in these types of cases—know in advance which sources of location data would ultimately be at issue. Rather, because GPS and CSLI are among the potential sources, the analytical assumption has to be that Location History records may be least as precise as the GPS or cell site signals in *Jones* and *Carpenter*.

II. The Third-Party Doctrine Does Not Diminish Mr. Chatrie's Expectation of Privacy in His Google Location Data.

The third-party doctrine does not apply to Location History records or diminish Mr. Chatrie's privacy interest in them. The doctrine generally holds that individuals do not have a reasonable expectation of privacy in information "voluntarily" conveyed to a third-party, but the *Carpenter* Court was clear that the rule is not to be "mechanically" applied in the digital age. 138 S. Ct. at 2219; *see also* ECF No. 29 at 9-11. Instead, *Carpenter* teaches that mobile location information is a "qualitatively different category" of data, distinct from the telephone numbers and bank records in *Miller*, 425 U.S. 435, or *Smith*, 442 U.S. 735. *See* 138 S. Ct. at 2216–17. The same reasoning applies here.

As Mr. Chatrie argues, "Google location records are qualitatively different from the business records to which the third-party doctrine traditionally applies." ECF No. 29 at 9. Unlike the numbers dialed in *Smith* or the bank deposit slips in *Miller*, Location History records are "detailed, encyclopedic, and effortlessly compiled," *Carpenter*, 138 S. Ct. at 2216, as well as deeply revealing. *See* ECF No. 29 at 12-13. Granting the government access to this information is

an unprecedented new surveillance power, akin to handing it a time machine capable of locating Google users in the past, all without expending finite physical resources like manpower or unmarked cars. *See id*. at 13-14. In short, it "gives police access to a category of information otherwise unknowable." *Carpenter*, 138 S. Ct. at 2218; *see also Prince Jones v. United States*, 168 A.3d 703, 714 (D.C. 2017) (use of a "cell site simulator" to locate a person through a cell phone is a search because the information is not readily available or in the public view, unlike visual surveillance or older generations of tracking devices).

The government counters that Mr. Chatrie has "voluntarily" shared this data with Google because Location History is an "opt-in service." *See* ECF No. 41 at 10-12. Google also describes "several steps" that a user must take in order for Location History to function and save information. ECF 96-1 at 2-3; ECF 59-1 at 12. But a closer look at this "opt-in" process reveals that it is not nearly as informed or voluntary as Google and the government suggest. On the contrary, users may unknowingly enable the function without ever seeing the phrase "Location History" or being informed of the privacy implications of turning it on. *See* ECF No. 72 at 6-9; 1/21/20 Tr. at 56-57.

Following the standard setup of an Android phone like the one used by Mr. Chatrie, a user encounters a pop-up screen, reproduced in *Figure 2*, when opening the Google Maps application for the first time. *See* ECF No. 72 at 7; 1/21/20 Tr. at 56. It says, "Get the most from Google Maps" and then it gives the user two options: "YES I'M IN" or "SKIP." *Id.* There is also a statement that reads "Google needs to periodically store your location to improve route recommendations, search suggestions, and more" and a button to "LEARN MORE." ECF No. 72 at 7. The pop-up does not use the phase "Location History," but clicking on "YES I'M IN" enables the function. Clicking on "LEARN MORE" takes the user to a webpage with Google's complete Privacy Policy and Terms

of Service; it does not direct the user to any specific language concerning location data or Location History specifically. *See* 1/21/20 Tr. at 57.

In fact, Google's Terms of Service do not mention Location History at all. *See* Google, Terms of Service (Oct. 25, 2017).[7] And Google's Privacy Policy, which is 27 pages long, mentions Location History only twice. *See* Google, Privacy Policy at 4, 8 (Jan. 22, 2019).[8] In the first

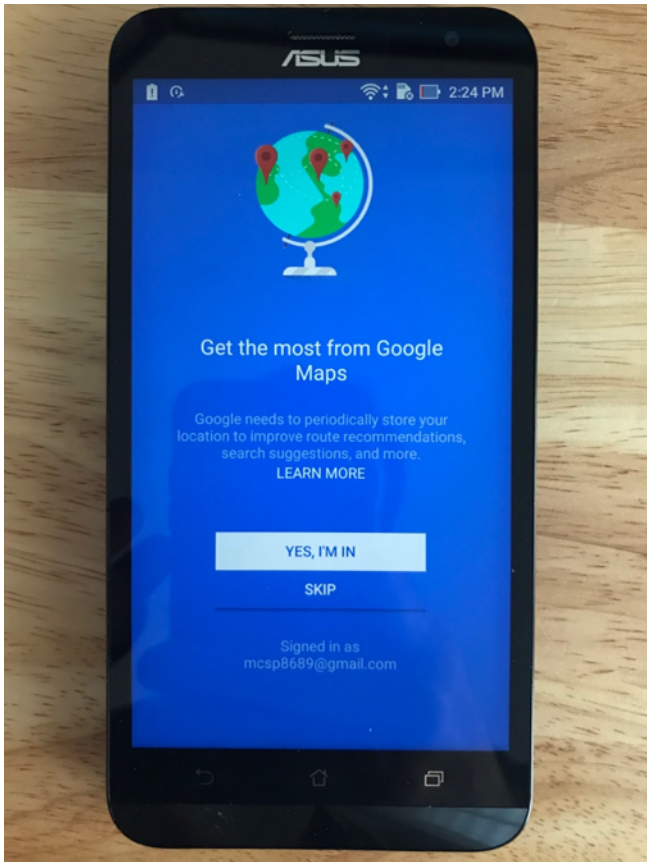

Figure 2

instance, it says, in full: "You can also turn on Location History if you want to create a private map of where you go with your signed-in devices." *Id.* at 4.[9] If anything, the phrase "private map"

[7] *Available at* https://policies.google.com/terms/archive/20171025.
[8] *Available at* https://www.gstatic.com/policies/privacy/pdf/20190122/f3294e95/google_privacy_policy_en.pdf.
[9] The Privacy Policy links to a current webpage with instructions on how to "Manage your Location History." The only date on the webpage is 2020 and it is not clear whether or what version of this page existed at the time Mr. Chatrie set up his phone.

is misleading and suggests that Google does not have access to the data. In the second instance, the policy says, in full: "Decide what types of activity you'd like saved in your account. For example, you can turn on Location History if you want traffic predictions for your daily commute, or you can save your YouTube Watch History to get better video suggestions." *Id*. at 8. Of course, "traffic predictions" do not begin to suggest that Google will keep a 24/7 "journal" of a user's whereabouts. But even if it did, a user would have no way of knowing that the pop-up "opt-in" screen relates to the Location History feature.

The pop-up does not reference "Location History" by name. As a result, a typical user would not know to scour Google's policies for references to Location History, much less understand the implications of the choice Google is asking them to make. In short, it is strikingly easy for a user to "opt-in" to Location History without ever being aware of doing so.

Consumer groups across Europe have filed complaints against Google over its location data practices, citing the deceptive design of the Location History "opt-in" process. *See Groups Across Europe File Complaints Against Google for Breach of GDPR*, The European Consumer Organisation (Nov. 27, 2018).[10] A complaint from Norway, for example, alleges that user consent to Location History tracking is not valid because it is not "freely given," "specific and informed," or "unambiguous." *Complaint to the Datatilsynet Under Article 77(1) of the European General Data Protection Regulation* at 8-12, Forbrukerrådet (Nov. 27, 2018).[11] Specifically, it argues that Location History can "be easily turned on involuntarily" and that the "relevant information regarding what Location History actually entails is hidden behind extra clicks and submenus, and the information about what the data is used for is ambiguous and unclear." *Id*. at 3, 11. It also

[10] *Available at* https://www.beuc.eu/publications/consumer-groups-across-europe-file-complaints-against-google-breach-gdpr/html.
[11] *Available at* https://fil.forbrukerradet.no/wp-content/uploads/2018/11/complaint-google-27-november-2018-final.pdf.

alleges that Google uses pop-up consent screens for Location History, similar to the one in Google Maps, in conjunction with other Google applications such as Google Assistant, the Google Search app, and Google Photos. *Id.* at 9. The cumulative effect is that a "user is repeatedly compelled to give consent using design patterns and biased notices," thereby increasing the likelihood that the user will "opt-in" by accident, out of frustration, or because of a belief that the services will not work otherwise. *Id*. In sum, "due to the deceptive design used by Google, it is not entirely clear for the user that she is actually giving consent to something, and even it was, it is not exactly clear to what she is consenting." *Id*. at 12; *see also Every Step You Take* at 16-23, Forbrukerrådet (Nov. 27, 2018) (the report on which the European complaints were based).[12]

On this side of the Atlantic, courts have been skeptical of so-called "clickwrap" contracts of adhesion. *See, e.g., Nguyen v. Barnes & Noble*, 763 F.3d 1171, 1175-76 (9th Cir. 2014) (categorizing "[c]ontracts formed on the Internet" as "clickwrap" or "browsewrap" depending on how they provide notice and seek assent); *Berkson v. Gogo*, 97 F. Supp. 3d 359, 395-401 (E.D.N.Y. 2015) (discussing "browsewrap," "clickwrap," "scrollwrap," and "sign-in-wrap"). Although the Fourth Circuit has not yet weighed in,[13] a recent opinion from this district is instructive. *See Melo v. Zumper*, No. 3:19-cv-621 (DJN), 2020 WL 465033, at *8-11 (E.D. Va. Jan. 28, 2020).

Like this case, *Zumper* involved a pop-up consent screen, but that is where the similarities end. The crucial question for the court in *Zumper* was "whether the website presented the terms

[12] *Available at* https://fil.forbrukerradet.no/wp-content/uploads/2018/11/27-11-18-every-step-you-take.pdf. The study's tests were performed "using a Samsung Galaxy S7 Android device running Android version 8.0.0" and then reproduced on a "Google Pixel device running Android 9." *Id.* at 6. While the "settings and device setup process may vary somewhat between devices," the results were "representative of a typical user experience." *Id*.; *see also* 1/21/20 Tr. at 36-37, 45-48 (discussing similarities in Location History prompts between Android versions).

[13] The Fourth Circuit in *A.V. ex rel. Vanderhye v. iParadigms*, LLC, 562 F.3d 630, 645 n.8 (4th Cir. 2009), "decline[d] to address the question of whether the terms of the Clickwrap Agreement created an enforceable contract."

and conditions in a hyperlink, and whether that hyperlink appeared clearly to the user." *Id.* at *9. In making this determination, the court considered the "placement of the terms and conditions hyperlink in relation to the button that grants a user access," "whether the terms and conditions hyperlink appeared to the user on multiple occasions," and "the overall design elements of the website, including font size and color, and other visual components that might hinder a user's reasonable notice." *Id.* at *9-10. In *Zumper*, the court concluded that the interface did provide sufficient notice of the company's terms and conditions because the company included a warning that "clearly stated that 'by creating a Zumper Account you indicate your acceptance of our Terms and Conditions and Privacy Policy," which were accessible through a conspicuous hyperlink directly below the "Create Account" button. *Id.* at *10-11.

In this case, by contrast, the "design and content" of Google's interface objectively obfuscates and discourages users from understanding what they are agreeing to. *See Berkson*, 97 F. Supp. 3d at 401. The pop-up here focused the user's attention on "get[ting] the most out of Google Maps" and did not mention Location History at all, let alone explain what clicking "YES, I'M IN" would entail. *See* Figure 2, *supra*; 1/21/20 Tr. at 56.

Mr. Chatrie would have had to agree to Google's terms and conditions during the initial setup process of his phone. *See* 1/21/20 Tr. at 50. But unlike the pop-up in *Zumper*, he did not have to view or assent to the terms again when he encountered the pop-up "opt-in" screen. He was not required to click through the text of Google's terms before Location History collection began; a renewed reference to the terms was not displayed, prominently or otherwise. *Cf. Tradecomet.com v. Google*, 693 F. Supp. 2d 370, 377-78 (S.D.N.Y. Mar. 5, 2010) (clickwrap agreement was reasonably communicated where the user "had to click through the text of that agreement" in order to agree"); *Moore v. Microsoft Corp.*, 293 A.D.2d 587, 587 (N.Y. 2002) (finding assent where the

terms were "prominently displayed on the program user's computer screen before the software could be installed" and the user was required to "click[] on the 'I agree' icon before proceeding with the download of the software."); *Feldman v. Google, Inc.*, 513 F. Supp. 2d 229, 237 (E.D. Pa. 2007) (finding notice and assent where "the user had to visit a webpage which displayed the Agreement in a scrollable text box," there was a "prominent admonition in boldface to read the terms and conditions carefully," and the terms were "only seven paragraphs long—not so long so as to render scrolling down to view all of the terms inconvenient or impossible"). The prompt did not even use the words "I Agree" or "Terms and Conditions," which may have at least implied that users were giving up something. *See* 1/21/20 Tr. at 56-57.

A "LEARN MORE" button is no substitute for a clear statement that users are agreeing to something drastically new. After all, the initial setup process—the point at which Mr. Chatrie did have to accept Google's terms—indicates that Location History is *not enabled* by default. *See* 1/21/20 Tr. at 53. Nothing about the pop-up screen indicates that users would be reasonably informed that they are changing this default setting or opting-in to the Location History service. Providing a link to all of Google's policies and terms of service is meaningless without a clear indication of what is changing and where to look.

III. The Geofence Warrant Infringed on Mr. Chatrie's Property Interests in His Location History Records and Was Therefore a Fourth Amendment Search.

Mr. Chatrie reiterates that he has a property interest in his Location History records, which constitute his private "papers and effects." *See* ECF No. 29 at 14-16; ECF No. 48 at 8-10. Google is a mere bailee of these records and the government can only search and seize them with a valid warrant. *See* ECF No. 29 at 15-16. The government has yet to address the substance of this argument, dismissing it as a theory "rooted in Justice Gorsuch's solo dissent in *Carpenter*," ECF No. 41 at 12. The government simply does not engage with centuries of Supreme Court

jurisprudence that embraces—and continues to validate—a property-based understanding of the Fourth Amendment. *See* ECF No. 48 at 8-10; *Carpenter*, 138 S. Ct. at 2213-2214 ("[N]o single rubric definitively resolves which expectations of privacy are entitled to protection"); *Jones*, 565 U.S. at 406-07 ("For most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates. *Katz* did not repudiate that understanding."); *id.* at414 ("*Katz*'s reasonable-expectation-of-privacy test augmented, but did not displace or diminish, the common-law trespassory test that preceded it.") (Sotomayor, J., concurring); *Kyllo*, 533 U.S. at 40 ("well into the 20th century, our Fourth Amendment jurisprudence was tied to common-law trespass").

Mr. Chatrie fully adopts, incorporates, and re-asserts his property-based arguments here. *See* ECF No. 29 at 14-16; ECF No. 48 at 8-10. If anything, Google's repeated insistence that Location History data is a personal "journal" only solidifies this claim, even if it is not a journal that users know they are keeping. *See* ECF No. 59-1 at 16; ECF No. 96-1 at 9. Regardless of whether the Court analyzes Mr. Chatrie's claim under a property-based theory or the reasonable expectation of privacy framework set forth in *Katz*, the result is the same. The search of Mr. Chatrie's Google Location History records was a Fourth Amendment search.

IV. The Geofence Warrant Was an Unconstitutional General Warrant, Fatally Overbroad and Lacking Particularity.

Mr. Chatrie also renews his argument that geofence warrants are inherently unconstitutional. They are the epitome of the indiscriminate, "dragnet"-style searches that the Supreme Court has repeatedly warned against—and that the Framers fought a revolution to prevent. *See* ECF No. 29 at 16-23. Indeed, the Supreme Court has never upheld anything remotely approaching the search of "numerous tens of millions" of people. *See* ECF No. 96-1 at 4. The new facts presented by Google in its *amicus* brief and affidavits only confirm that the warrant in this

case was uniquely overbroad and so lacking in particularity that it can only be described as the digital equivalent of an impermissible general warrant.

A. Overbreadth

The geofence warrant here did not—and could not—meet the probable cause or particularity requirements demanded by the Fourth Amendment. It did not identify any individuals or accounts to be searched because investigators did not know who they were searching for, or even if Google would have relevant data. *See* ECF No. 29 at 23. Nothing in the warrant application indicates that the bank robber was a Google user or had Location History enabled at the time of the robbery. *Id*. Instead, the application rested on broad conjecture based on the popularity of Google and cell phones generally. *See* ECF No. 29 at 23; ECF No. 48 at 19.

From the outset, the government enlisted Google to search untold *millions* of unknown accounts in one of the largest fishing expeditions in Fourth Amendment history. The number of individuals affected by this case dwarfs the number of people searched in any other reported criminal opinion. Even controversial "tower dumps," which are exceedingly broad in their own right, tend to impact hundreds or thousands of people at most. *See, e.g., United States v. James*, No. 18-CR-216, 2019 WL 325231, at *3 (D. Minn. Jan. 25, 2019) ("hundreds if not thousands" of cell phone users); *In re Cell Tower Records Under 18 U.S.C. 2703(D)*, 90 F. Supp. 3d 673, 676 (S.D. Tex. 2015) ("several thousand phone numbers"); *United States v. Pembrook*, 119 F. Supp. 3d 577, 586 (E.D. Mich. 2015) ("potentially hundreds"); *In re Application of the U.S.A. for an Order Pursuant to 18 U.S.C. 2703(c), 2703(d)*, 42 F. Supp. 3d 511, 513 (S.D.N.Y. 2014) ("hundreds or thousands"); *In re Search of Cellular Tel. Towers*, 945 F. Supp. 2d 769, 770 (S.D. Tex. 2013) **("**hundreds, or even thousands").

A tower dump requires cell phone service providers to produce the records of every device connected to a particular cell tower or towers during a particular time. *See* ECF 59-1 at 14. But as a practical matter, the number of people affected is limited by the number of cell phone users who were present at the time—*i.e.*, hundreds or thousands, depending on the area and the time. The difference with geofence searches is that there is no such practical upper limit. Rather, Google asserts that it has "no way to identify which of its users were present in the area of interest without searching the [Location History] information stored by every Google user." *Id*. Consequently, the number of users searched using a geofence warrant is bound only by the number of Google users with Location History enabled, which Google estimates to be in the "numerous tens of millions." ECF No. 96-1 at 4.

The government cites to the "Playpen" cases as a justification for the breadth of the search here. *See* ECF No. 41 at 19-20. Those cases arose from a warrant that searched users who logged into a child pornography website temporarily run by the FBI. The scheme was one of the largest sting operations in history, but it still only involved "approximately nine thousand" computers globally. *See* Order on Defendants' Motion to Dismiss Indictment at 5, 12, *United States v. Tippens*, No. 16-05110-RJB (W.D. Wash. Nov. 30, 2016) (ECF No. 106). Moreover, users had to take numerous affirmative steps to access and log into the website, making it "extremely unlikely for someone to stumble innocently upon Playpen." *United States v. Matish*, 193 F. Supp. 3d 585, 603 (E.D. Va. 2016); *see also United States v. McLamb*, 880 F.3d 685, 688 (4th Cir. 2018) (noting that in order to access Playpen, a user must download special software and enter a 16-character URL consisting of random letters and numbers, as well as enter a username and password to proceed past a welcome page that "was suggestive enough that Playpen's content would be apparent" to any visitor). By contrast, there was no government honeypot in this case, and there is

no argument that using Location History or being near the Call Federal Credit Union is inherently suspicious. *See* ECF No. 48 at 13.

The fact that Google produced the records belonging to 19 of these users does not diminish the scope of the initial search conducted at the government's behest. Unlike scenarios where a company must search defined records to identify responsive data, the search here did not identify any specific users or accounts to be searched. Instead, the warrant forced Google to act as an adjunct detective, scouring the accounts of numerous tens of millions of users with Location History enabled in order to generate a lead for the government. That the intimate, private data of numerous tens of millions of users were searched is the heart of the overbreadth analysis in this case. That records belonging to 19 people were ultimately produced does not lessen the massive, and illegal, search conducted in this case.

B. Particularity

A geofence warrant is overbroad by design, but it is also severely lacking in particularity. Apart from probable cause, the Fourth Amendment requires that warrants "particularly describ[e]" the place to be searched and the things to be seized. U.S. Const. amend. IV. The idea is to leave nothing to the discretion of the officers executing a warrant that a court has properly authorized. *See Marron v. United States*, 275 U.S. 192, 196 (1927). This is especially critical where, as here, a search implicates First Amendment concerns. *See* ECF No. 29 at 13, 22; ECF No. 48 at 3 n.3. If particularized, it should be obvious to all what officers can search and what they can seize. The exact opposite occurred here.

The geofence warrant left it up to Google and the government to negotiate which users would have their account information searched and further revealed to investigators—the hallmark of an unparticularized warrant. *See Steagald v. United States*, 451 U.S. 204, 220 (1981); *Stanford*

v. Texas, 379 U.S. 476, 482-83 (1965) (describing the "battle for individual liberty and privacy" as finally won when British courts stopped the "roving commissions" given authority to "search where they pleased"). As Mr. Chatrie contends, "a three-step, back-and-forth process with the recipient of a warrant is not a substitute for particularizing that warrant at the outset. Instead, it is an unconstitutional delegation of discretion to the executing officers." ECF No. 29 at 23. At each step along the way, Google and the government—not the issuing magistrate—decided what data to search and what data to produce. Even the government now appears to agree that there was some "lack of clarity about what this search warrants asks for." 1/21/20 Tr. at 171.

At Step One, Google made critical decisions that would ordinarily be made by a judge, not the recipient of the warrant. First, Google decided to search only a portion of its records, specifically "Location History" records kept in the "Sensorvault." *See* ECF No 96-1 at 3. Google then decided to ignore the margins of error generated by its own calculations and "estimate" that 19 Google users were within the 150-meter geofence. In reality, at least five of those 19 users were never within the geofence at all.[14] Instead, Google guessed—inaccurately. One device could have been more than 387 meters away from the bank, and yet Google still identified its user as a potential suspect subject to additional search in Step Two.

During Step Two, the warrant said the government would "attempt" to narrow the Step One returns and then obtain additional location information on a subset of devices of interest. *See* ECF No. 54-1, Attach. I at 1-2; Attach. II at 2-3. The government did not try very hard. Instead, the government approached Google multiple times to press for expanded data on all 19 of the devices identified in Step One. First, Detective Hylton emailed Google on or about July 2, 2019, to request "additional location data (*i.e.*, step 2) and subscriber information (*i.e.*, step 3) for all 19

[14] Device IDs 702354289, -965610516, 907512662, 1135979718, and 2021066118.

device numbers produced in step 1." ECF No. 96-2 at 5; *see also* ECF No. 48 at 14, Ex. A at 1. On July 8, Det. Hylton called Google twice, and left two voicemails, presumably requesting the same. *Id*. A Google representative called Det. Hylton back and "explained the issues in the Detective's email as the request did not appear to follow the three sequential steps or the narrowing required by the search warrant." *Id*. Google also "explained the importance of step 2 in narrowing" to Det. Hylton. *Id.* At some point, the government emailed Google once again to ask for "additional location data and subscriber info" on all 19 devices identified in Step One. *See* ECF No. 48, Ex. B at 1.[15] In each email, Det. Hylton wrote to Google that, "If this request seems unreasonable, please keep in mind that device numbers 1-9 may fit the more likely profile of parties involved," but proceeded to request additional information on all 19 users anyway. *See* ECF No. 48, Ex. A at 1; *id.*, Ex. B at 1. Eventually, Det. Hylton acquiesced and emailed Google a third time to request additional information on 9 of the 19 users. *Id.*, Ex. C at 1. The third time around, Google complied.

The haggling between Google and Det. Hylton is emblematic of the absence of particularity in the geofence warrant. The Fourth Amendment demands that a neutral and detached magistrate make decisions about what to search and what to seize. This constitutional function cannot be outsourced to Google or to the police. As well-intentioned as Google may be, it is not up to Silicon Valley to determine what is "reasonable." *Cf.* ECF No. 48, Ex. A at 1; *id.*, Ex. B at 1 ("If this request seems unreasonable…"). That decision belongs to the judicial branch, and the judicial branch only. *See Groh v. Ramirez*, 540 U.S. 551, 561 (2004) ("Even though [law enforcement] acted with restraint in conducting the search, 'the inescapable fact is that this restraint was imposed by the agents themselves, not by a judicial officer.'") (quoting *Katz*, 389 U.S. at 356).

[15] The government has not provided the dates for either of the emails to Google.

Furthermore, a basic premise of the warrant was that the data returns in Step One and Step Two would be "anonymized." But as Mr. Chatrie has consistently argued, "[t]he fact that Google masks the true 'Device ID' with a pseudonym does not make the data anonymous." *See* ECF No. 68 at 3; ECF No. 72 at 10; 1/21/20 Tr. at 83, 87-88, 90-91. On the contrary, every person takes a "unique path through life" that is "inherently identifiable." ECF No. 68 at 3; *see also* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701, 1716 (2010). And as Mr. Chatrie demonstrated, the impossibility of anonymizing location data holds true in this case as well. *See* 1/21/20 Tr. at 83, 87-88, 90-91. It is trivial to plot "anonymized" coordinates on a map, connect the dots, and determine which house belongs to whom. *See* ECF No. 68 at 3; 1/21/20 Tr. at 74-75. Indeed, the Step One returns may be enough, without anything more from Google, for law enforcement to determine the identity of "anonymized" users. *See* 1/21/20 Tr. at 86-87.[16] Consequently, this Court "should not discount the intrusiveness of the initial data returns disclosed by Google." ECF No. 72 at 10.

In Step Three, the government selected three Google users for even further scrutiny. At least one of these users[17] was likely never inside the geofence at all, something which should have been apparent to investigators reviewing the Step Two returns. Nonetheless, the government decided to have Google de-anonymize this user's records and turn over additional subscriber information associated with the account.

[16] For this reason, Mr. Chatrie does not believe it is appropriate, as the government suggests, to sever the warrant and consider Step One separately from Step Two. *See* ECF No. 41 at 20. Furthermore, doing so would "condone the digital equivalent of a general warrant that lacked particularity from the outset." ECF No. 48 at 14 n.5; *see also United States v. Sells*, 463 F.3d 1148, 1158 (10th Cir. 2006) (noting that "every court to adopt the severance doctrine has further limited its application to prohibit severance from saving a warrant that has been rendered a general warrant by nature of its invalid portions despite containing some valid portion").

[17] Device ID: 907512662.

At no point during this three-step process did the government return to the magistrate to seek further authorization. *See* ECF No. 29 at 23-24. Instead, it was up to Google to determine what was "reasonable," beginning with the scope of the initial search, and including the returns provided in Steps Two and Three. ECF No. 48, Ex. A at 1; *id.*, Ex. B at 1. The point is not that Google should have searched the Location Accuracy or Web & App Activity databases, or that Google should have produced more or less records. The point is that this is not how warrants are supposed to work. What the government can search and seize is a question that the Constitution reserves for the judiciary, not for Google or the police. *See Groh*, 540 U.S. at 561 ("Even though [law enforcement] acted with restraint in conducting the search, 'the inescapable fact is that this restraint was imposed by the agents themselves, not by a judicial officer.'") (quoting *Katz*, 389 U.S. at 356); ECF No. 48 at 15-16. The delegation of this authority to Google only demonstrates the profound lack of particularity in the geofence warrant. *See* ECF No. 48 at 16.

V. The Good Faith Exception Does Not Apply.

Mr. Chatrie fully adopts, incorporates, and re-asserts in this supplement that the *Leon* good faith exception to the exclusionary rule does not apply to evidence obtained from a warrant that was *void ab initio*. *See* ECF No. 48 at 17-20. As set forth above and in the original geofence warrant briefing, this geofence warrant is void from its inception and thus, is no warrant at all. *See United States v. Krueger*, 809 F.3d 1109, 1123-24 (10th Cir. 2015) (Gorsuch, J., concurring); *see also Groh*, 540 U.S. at 558 ("[T]he warrant was so obviously deficient that we must regard the search as 'warrantless' within the meaning of our case law.").

Of critical importance here is the omission of key facts in the warrant affidavit that should have flagged the unique overbreadth of the search for the reviewing magistrate—namely, the true scope of the number of people to be searched and the true boundaries of the "geofence." Had the

magistrate known that the warrant he signed authorized Google to search the private daily journals of numerous tens of millions of people, surely he would have refused to sign such a warrant. Had the magistrate known that the warrant he signed simultaneously authorized a search of a church, a hotel, a restaurant, a mini storage facility, and two apartment complexes, surely he would have laid his pen on his desk and sent the affiant away empty-handed. To not include those facts demonstrates at least recklessness with regard to the true nature of the search the affiant proposed.

The unprecedented search of numerous tens of millions of private diaries at once also renders the warrant so overbroad that no reasonably objective officer would have thought it a valid warrant. *See, e.g., United States v. Winn*, 79 F. Supp. 3d 904, 923-24 (S.D. Ill. 2015) (refusing to find good faith where two officers had fifteen years of experience between them and obtained a warrant that "gave them unbridled discretion to search for and seize whatever they wished"). In *Winn*, officers used a template affidavit that received only a "quick and cursory" review by the State's Attorney to obtain "any or all files" on an individual's cell phone. *Id*. at 919, 923-24. While consultation with counsel was "prima facie evidence" of good faith, the court found that *Leon* did not apply because of the government's "recklessness" as to particularity. *Id*. at 923. The court also found that the judge "did the same . . . abandon[ing] his judicial role to some extent" by authorizing "a warrant to rummage through every conceivable bit of data." *Id*. at 923-24. Such disregard for the particularity requirement negated the government's claim of good faith in *Winn*, *id.* at 924, and it should have the same result here.

In this case the government used a warrant template (the provenance of which is still unclear to Mr. Chatrie) that was fundamentally overbroad and lacking in particularity. It substituted generalized assumptions about cell phone use for probable cause and sought to authorize the unbridled search of numerous tens of millions of Google users. It did not even attempt

to exclude devices associated with the Journey Christian Church any step along the way. The government then presented this application to a state magistrate who approved it without any information or, presumably, understanding of the scope of the search or the level of discretion being afforded to investigators. As in *Winn*, such reckless disregard for the probable cause and particularity requirements should negate the government's argument that it acted in good faith. *See also United States v. Doyle*, 650 F.3d 460, 476 (4th Cir. 2011) ("[W]here a reasonable officer would know that a probable cause determination could not be rendered without information conspicuously absent from his application for a warrant, reliance on the resulting warrant is not objectively reasonable.").

CONCLUSION

The geofence warrant here was the epitome of a general warrant, a search of numerous tens of millions of Google users in an attempt to develop a single lead. Its overbreadth and absence of particularity are so unprecedented that no officer would reasonably rely on it. As a result, this Court should suppress all evidence and fruits that the government obtained from it.

Respectfully submitted,
OKELLO T. CHATRIE

By: _____/s/_____
Michael W. Price
NY Bar No. 4771697 (*pro hac vice*)
NACDL, Fourth Amendment Center
1660 L St. NW, 12th Floor
Washington, D.C. 20036
Ph. (202) 465-7615
Fax (202) 872-8690
mprice@nacdl.org

_____/s/_____
Laura Koenig
Va. Bar No. 86840
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0881
Fax (804) 648-5033
laura_koenig@fd.org